PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, G11B 20/00

A1

(11) International Publication Number: **WO 98/52114**

(43) International Publication Date: 19 November 1998 (19.11.98)

(21) International Application Number: PCT/US98/08422

(22) International Filing Date: 6 May 1998 (06.05.98)

(30) Priority Data:
08/857,235 16 May 1997 (16.05.97) US

(71) Applicant: IMATION CORP. [US/US]; 1 Imation Place, P.O. Box 64898, Saint Paul, MN 55164-0898 (US).

(72) Inventor: BLIXT, Jon, J.; P.O. Box 64898, Saint Paul, MN 55164-0898 (US).

(74) Agents: LEVINSON, Eric, D. et al.; Imation Legal Affairs, P.O. Box 64898, Saint Paul, MN 55164-0898 (US).

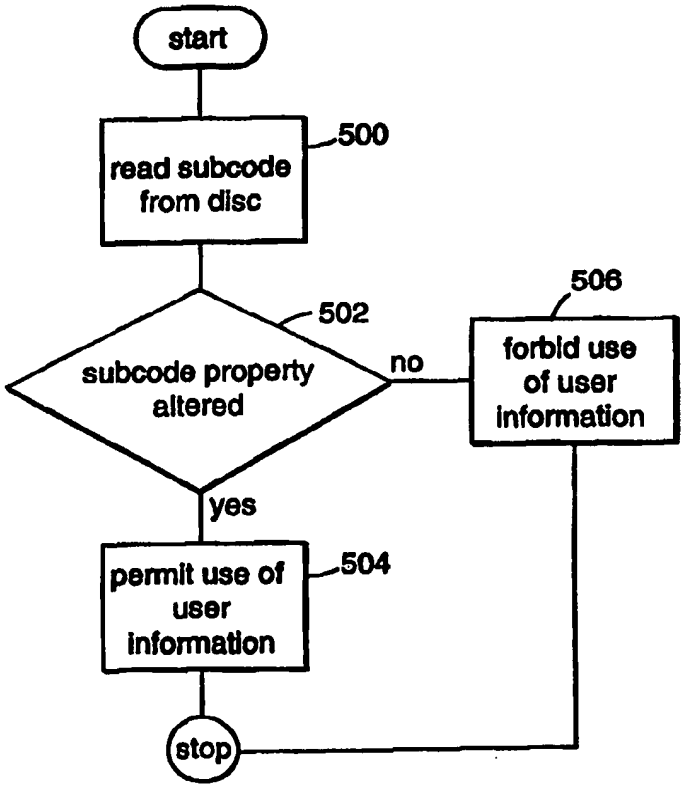
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ARRANGEMENT FOR PREVENTING USE OF UNAUTHORIZED DUPLICATES OF A DATA STORAGE MEDIUM USING SUBCODE AND METHOD THEREFOR

(57) Abstract

A copy-protection method includes modifying portions of the subcode (216) on a disc (100). The modified subcode is normally disregarded when reading the disc and is not copied during typical copying operations. When a user wishes to execute a program stored on the disc using a computer, the computer determines (502) whether the subcode is modified. If the subcode contains certain data, the user is permitted (504) to execute the program. Otherwise, the user is prevented (506) from executing the program.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

ARRANGEMENT FOR PREVENTING USE OF UNAUTHORIZED DUPLICATES OF A DATA STORAGE MEDIUM USING SUBCODE AND METHOD THEREFOR

Field of the Invention

The present invention relates to data storage. More particularly, the present invention relates to preventing use of unauthorized copies of a data storage medium.

Background of the Invention

Optical media, such as discs recorded in the Compact Disc-Read Only Memory (CD-ROM) format, have become a popular data storage medium for storing computer software. Their large storage capacity allows them to store programs that are too large to be stored practically on certain other types of removable media, such as magnetic media known as floppy disks. For example, CD-ROMs are capable of storing video clips and CD-quality audio clips.

The proliferation of optical recording devices and writable optical media in the consumer market has facilitated storage of data on CD-ROMs. Decreasing prices of both optical recording devices and writable optical media have given an increasing number of consumers access to this technology. As a result, unauthorized duplication of CD-ROMs is a significant concern in the software industry.

Several techniques have been proposed to prevent unauthorized duplication of optical media. Some of these techniques involve using certain codes that identify an optical medium as an original. These techniques can be defeated using an approach known as sequential copying, in which the data on an optical medium is read sequentially and copied to a writable optical medium. Using sequential copying, an optical recording device can make a copy of an optical medium

that is indistinguishable from the original. In addition, many such techniques involve using circuitry to detect the codes. Optical recording devices that lack this detection circuitry can copy optical media despite the presence of the codes.

Some other copy protection techniques involve physically altering the original medium to render areas of the medium difficult to read and copy by an optical reading device. An optical recording device can, however, copy the original medium by skipping over these areas. Because the original medium is physically altered, identifying the altered areas of the original medium is relatively easy. Furthermore, physical alterations can cause inconsistencies in playback from different optical reading device manufacturers. To prevent these inconsistencies, these techniques often use areas known as buffer zones to increase the error tolerance of the medium. These buffer zones use part of the user space on the medium and thus reduce the amount of space that can store other information.

Summary of the Invention

According to one embodiment, the present invention is directed to a method for use in preventing use of unauthorized duplicates of an original data storage medium storing user information. The method includes providing an original data storage medium having a plurality of first segments for storing the user information and a plurality of second segments for storing format information that is disregarded during a processing mode of a data storage medium reading device. Selected data is stored on at least one of the second segments. The data storage medium reading device reads said at least one of the second segments and determines whether to allow or prevent use of the user information as a function of whether said at least one of the second segments contains the selected data.

Additional embodiments are directed to apparatuses for performing this method and to a method in which a computer-executable program is stored on the original data storage medium. The other computer-executable program, when executed, commands the data storage medium reading device to read said at least one of the second segments, and determines whether to allow or prevent use of the user information as a function of whether said at least one of the second segments contains the selected data.

Still another embodiment of the present invention is directed to a data recording apparatus for use in preventing use of unauthorized duplicates of a data storage medium storing user information. The data storage apparatus comprises an encoding arrangement, coupled to receive a data stream and configured and arranged to encode the data stream as a modulated data stream. The encoding arrangement is also configured and arranged to generate nonstandard format information. A controller responsive to the encoding arrangement generates a control signal at least in part as a function of the modified format information and the modulated data stream. The control signal controls a modulator that modulates a laser beam generated by an oscillator.

Another embodiment of the present invention is directed to a data storage medium that has a plurality of first segments storing user information and a plurality of second segments storing format information. During a processing mode of a data storage medium reading device, the format information is disregarded. At least a portion of the format information contains certain data if the data storage medium is an original data storage medium. The data storage medium stores a computer-executable program. The computer-executable program, when executed, commands the data storage medium reading device to read

at least one of the second segments, and determines whether to allow or prevent use of the user information as a function of whether said at least one of the second segments contains the certain data.

According to another aspect of the present invention, an authentication method comprises commanding a data storage medium reading device to read a portion of a data storage medium. The portion contains nonstandard format information if the data storage medium is an original data storage medium. The method also includes determining whether to allow or prevent use of user information stored on the data storage medium as a function of whether the format information is nonstandard.

The above summary of the invention is not intended to describe each disclosed embodiment of the present invention. This is the purpose of the figures and of the detailed description that follows.

Brief Description of the Drawings

Other aspects and advantages of the present invention will become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 is a plan view of an optical data storage medium, according to the present invention, illustrating logical structures for storing data;

FIG. 2A is a diagram conceptually illustrating an example data format for storing data on the optical data storage medium of FIG. 1, according to the present invention;

FIG. 2B is a diagram conceptually illustrating another example data format for storing data on the optical data storage medium of FIG. 1, according to the present invention;

FIG. 3 is a block diagram of an optical recording device for recording data on the optical data

storage medium of FIG. 1, according to the present invention;

FIG. 4 is a flow chart of a method for preventing unauthorized duplication of an optical data storage medium, according to the present invention; and

FIG. 5 is a flow chart of a method for authenticating an optical data storage medium, according to the present invention.

Detailed Description of the Various Embodiments

The present invention is believed to be applicable to a variety of systems and arrangements that prevent the use of unauthorized copies of optical storage media. The invention has been found to be particularly advantageous in application environments in which a CD-ROM or other optical medium stores user information, such as a computer-executable program for use by a personal computer (PC) or other computer arrangement. An appreciation of various aspects of the invention is best gained through a discussion of various application examples operating in such an environment. While the examples are discussed in the context of the CD-ROM format, it should be understood that the techniques described can be adapted readily to a variety of optical storage formats. Examples of such formats include, but are not limited to, the Digital Video Disc - Read Only Memory (DVD-ROM), CD-Erasable (CD-E), and CD-Recordable (CD-R) formats.

FIG. 1 illustrates a CD-ROM 100 that includes a reflective substrate on which information is stored as pits in the substrate and lands between the pits. The pattern of pits and lands represents the information stored on the CD-ROM 100. Any of a variety of techniques, including, for example, conventional photoresist techniques, can be used to create the pits. The CD-ROM 100 includes a center aperture 102 to

facilitate placement of the CD-ROM 100 in an optical reading device, such as a CD-ROM drive.

The CD-ROM 100 physically consists of a single spiral track from the inner perimeter of the CD-ROM 100 to an outer perimeter of the CD-ROM 100. While the spiral track is typically considered a single logical segment, the spiral track can be further divided into a plurality of logical segments 104, which are exaggerated on FIG. 1 for illustration purposes. The logical segments 104 are further divided into sectors 106. The sectors 106 are also exaggerated on FIG. 1 for illustration purposes.

FIGS. 2A and 2B illustrate two example sector formats, according to the CD-ROM standard. FIG. 2A illustrates a sector format known as Mode 1. A Mode 1 sector includes twelve bytes comprising a synchronization section 202. A header section 204 consists of four bytes. The header section 204 is followed by a user data section 206 that stores user information, such as program data, image data, or audio data. The user data section 206 is 2048 bytes long in a Mode 1 sector. A four-byte error detection code (EDC) 208 and an eight-byte reserved section 210 follow the user data section 206. The reserved section 210 is typically blank. A 276-byte error correction code 212 follows the reserved section 210 and provides enhanced error correction. An error detection/error correction (ED/EC) section 214 follows the error correction code 212 and provides basic error detection and correction functions. Those skilled in the art will appreciate that the above-described sections are typically physically interleaved to improve error tolerance. In the CD-ROM format, each 2352-byte sector is divided into ninety-eight interleaved 24-byte frames. Each frame is followed by one byte of subcode. The subcode bytes, when combined, comprise a 98-byte subcode section 216 that contains formatting information. In

the audio CD format, the formatting information includes time index and audio track, *e.g.*, song information.

In the CD-ROM format, an optical reading device addresses sectors of the CD-ROM using an index known as absolute time or ATIME. Absolute time identifies time indexes from the beginning of the disc, using an internal clock of the optical reading device. Because optical reading devices compliant with the CD-ROM standard use absolute time to address sectors of the CD-ROM, the formatting information stored in the subcode section 216 is not used during normal read operations of the optical reading device or CD-ROM drive.

FIG. 2B illustrates a CD-ROM sector format known as Mode 2. The Mode 2 format is similar to the Mode 1 format. In the Mode 2 format, however, the EDC section 208, the reserved section 210, and the ECC section 212 are absent. The space conserved by omitting these sections stores additional user data. Accordingly, the user data section 206 is 2336 bytes long in the Mode 2 format.

To prevent the use of user information, such as software, on an unauthorized copy of an original CD-ROM, according to the present invention, a manufacturer alters at least some of the subcode areas on the CD-ROM. Because the subcode areas do not store user information and are not normally read by the CD-ROM drive, the alterations to the subcode areas do not affect program data or other user information. A purchaser of an original CD-ROM can thus use software stored on the CD-ROM normally. Because CD-ROM drives do not normally read the subcode areas, however, the altered subcode is not copied during normal copying operations. Copies of an original CD-ROM made by typical optical recording devices therefore do not contain the modified subcode.

The CD-ROM stores an authentication program that, when executed, commands the CD-ROM drive to read the subcode areas. The authentication program allows use of the user information stored on the CD-ROM only if the subcode areas are properly altered, indicating that the CD-ROM is an original. Authenticating the CD-ROM as an original using an authentication program allows any CD-ROM drive to authenticate the CD-ROM, regardless of whether the CD-ROM drive has detection circuitry configured to detect the modified subcode.

Because the subcode alterations do not alter the user data and are not normally read by a CD-ROM drive, detecting the copy protection is difficult. A user can copy the original CD-ROM easily, but cannot execute a program stored on a copy of the CD-ROM. No record of the subcode alterations exists, rendering detection of the alteration difficult, unless an end user inspects a large number of data blocks, *e.g.*, over 300,000, by analyzing certain CD-ROM information that is not normally provided to the end user. Furthermore, the particular subcode areas that are altered can be randomly varied between individual CD-ROMs. In this manner, a CD-ROM manufacturer can discourage even facilities that have equipment that are capable of producing usable copies of originals protected according to the present invention from producing unauthorized copies of multiple CD-ROMs. Even if such a facility can defeat the copy protection for a particular CD-ROM, defeating the copy-protection for another CD-ROM involves thorough analysis of the CD-ROM.

FIG. 3 is a block diagram of an optical recording device, according to the present invention, used in producing a copy-protected CD-ROM. A digital data stream 300, such as program information for a computer application, is provided to an encoder 302. For example, one type of encoder commonly used in

recording data on CD-ROMs is known as an 8-to-14 modulation (EFM) encoder. Encoders of this type encode data streams having eight-bit bytes, which are commonly used to store data on magnetic media, to a data stream having fourteen-bit bytes. Optical storage media typically use fourteen-bit bytes to allow encoding of two consecutive ones using pits and lands. During read operations of a CD-ROM drive, an interface card converts the fourteen-bit code back to the eight-bit code used by the computer.

A subcode generator 304 provides subcode to a computer arrangement 306, including, for example, a CPU. The computer arrangement 306 is implemented using, for example, a conventional personal computer (PC) or a group of computers. The subcode generator 304 can be implemented using a distinct component, as illustrated, or integrated as part of the computer arrangement 306. For example, the subcode generator 304 and the encoder 302 can be implemented using a single card installed on a computer. The subcode is generated in a form inconsistent with typical formats, *e.g.*, containing unexpected data. The computer arrangement 306 interleaves the modified subcode and the encoded data stream and generates a recording signal.

A modulator controller 308 receives the recording signal and generates a control signal used for controlling a modulator 310. The modulator 310 modulates the intensity of a continuous-intensity laser beam generated by an oscillator 312. Accordingly, the modulator 310 produces a laser beam having a modulation that varies as a function of the recording signal. An objective lens 314 focuses the modulated laser beam on a location of a CD-ROM or a master used for producing CD-ROMs.

FIG. 4 is a flow chart illustrating an example method for preventing use of unauthorized

copies of an original CD-ROM, according to the present invention. As depicted at a block 400, an encoder reads source data, such as software code. The encoder provides the source data and other encoded information to a computer arrangement. The computer arrangement generates subcode, as depicted at a block 402. At least part of the subcode is nonstandard. The source data and subcode are interleaved and written to a CD-ROM, as respectively depicted at blocks 403 and 404.

At a block 406, an authentication program is stored. The authentication program allows use of user information, such as software, stored on the CD-ROM only if the modified subcode areas are present on the CD-ROM. Absence of the modified subcode areas indicates that the CD-ROM is an unauthorized copy. Accordingly, the authentication program prevents use of the user information stored on the CD-ROM if the modified subcode areas are absent. Alternatively, the authentication program can be incorporated into another application program stored on the CD-ROM. The authentication program can also be interleaved with the source data and subcode instead of being written to the CD-ROM in a separate process.

FIG. 5 is a flow chart illustrating an example of the operation of the authentication program. At a block 500, the authentication program commands the CD-ROM drive to read the subcode areas of the CD-ROM. The authentication program then determines whether the subcode areas are properly altered, as depicted at a block 502. If the subcode areas are altered properly, the authentication program permits use of user information stored on the CD-ROM, as depicted at a block 504. On the other hand, if the subcode areas are not properly altered, the authentication program prevents the user from using the user information, as depicted at a block 506. Because it is difficult to determine why the copy of the CD-ROM does not work or

the portions of the CD-ROM that were not copied, circumventing this copy protection scheme is difficult.

What is claimed is:

1. For use in preventing use of unauthorized duplicates of an original data storage medium (100) storing user information, a copy-protection method comprising:

providing an original data storage medium having a plurality of first segments (206) for storing the user information and a plurality of second segments (216) for storing format information that is disregarded during a processing mode of a data storage medium reading device;

storing (404) selected data on at least one of the second segments;

commanding (500) the data storage medium reading device to read said at least one of the second segments; and

determining (502) whether to allow (504) or prevent (506) use of the user information as a function of whether said at least one of the second segments contains the selected data.

2. The method of claim 1, further comprising storing the user information and the format information in one of the following formats: CD-ROM, DVD-ROM, CD-E, and CD-R.

3. The method of claim 1, wherein the second segments contain subcode.

4. The method of claim 1, further comprising creating a master for providing the original data storage medium.

5. The method of claim 1, further comprising randomly selecting said at least one of the second segments for storing the selected data.

6. For use in preventing use of unauthorized duplicates of a data storage medium (100) storing user information, a data storage apparatus comprising:

an encoding arrangement (302) coupled to receive a data stream (300) and configured and arranged to:

encode the data stream as a modulated data stream, and

generate nonstandard format information;

an oscillator (312) configured and arranged to generate a laser beam;

a modulator (310) responsive to a control signal and configured and arranged to modulate the laser beam; and

a controller (308) responsive to the encoding arrangement and configured and arranged to generate the control signal at least in part as a function of the nonstandard format information and the modulated data stream.

7. The apparatus of claim 6, wherein the format information comprises subcode.

8. The apparatus of claim 6, wherein the encoding arrangement is further configured and arranged to generate a second data stream as a function of the received data stream and the nonstandard format information.

9. The apparatus of claim 6, wherein a microprocessor (306) is further configured and arranged to command the modulator to modulate the laser beam for storing an authentication program (406) on the data

storage medium, and wherein the authentication program is configured and arranged to, when executed,

command (500) a data storage medium reading device to read a portion of the data storage medium, and

determine (502) whether to allow (504) or prevent (506) use of the user information as a function of whether the format information is modified.

10. The apparatus of claim 6, further comprising a lens (314), configured and arranged to focus the laser beam on a portion of the data storage medium.

11. For use in preventing use of unauthorized duplicates of an original data storage medium (100) storing user information, an authentication method comprising:

commanding (500) a data storage medium reading device to read a portion of the data storage medium, the portion containing nonstandard format information (216) if the data storage medium is the original data storage medium; and

determining (502) whether to allow (504) or prevent (506) use of the user information as a function of whether the format information is nonstandard.

12. The method of claim 11, wherein the format information comprises subcode.

13. An optical data storage disc (100), comprising:

a plurality of first segments (206) for storing user information;

a plurality of second segments (216) for storing format information that is disregarded during a processing mode of an optical data storage disc reading device, at least a portion of the format information

containing certain data if the data storage disc is an original data storage disc; and

a computer-executable program (406), configured and arranged to, when executed,

command (500) the data storage disc reading device to read at least one of the second segments, and

determine (502) whether to allow (504) or prevent (506) use of the user information as a function of whether the format information contains the certain data.

14. The disc of claim 13, wherein the format information comprises subcode, and wherein the computer-executable program comprises a portion of the user information.

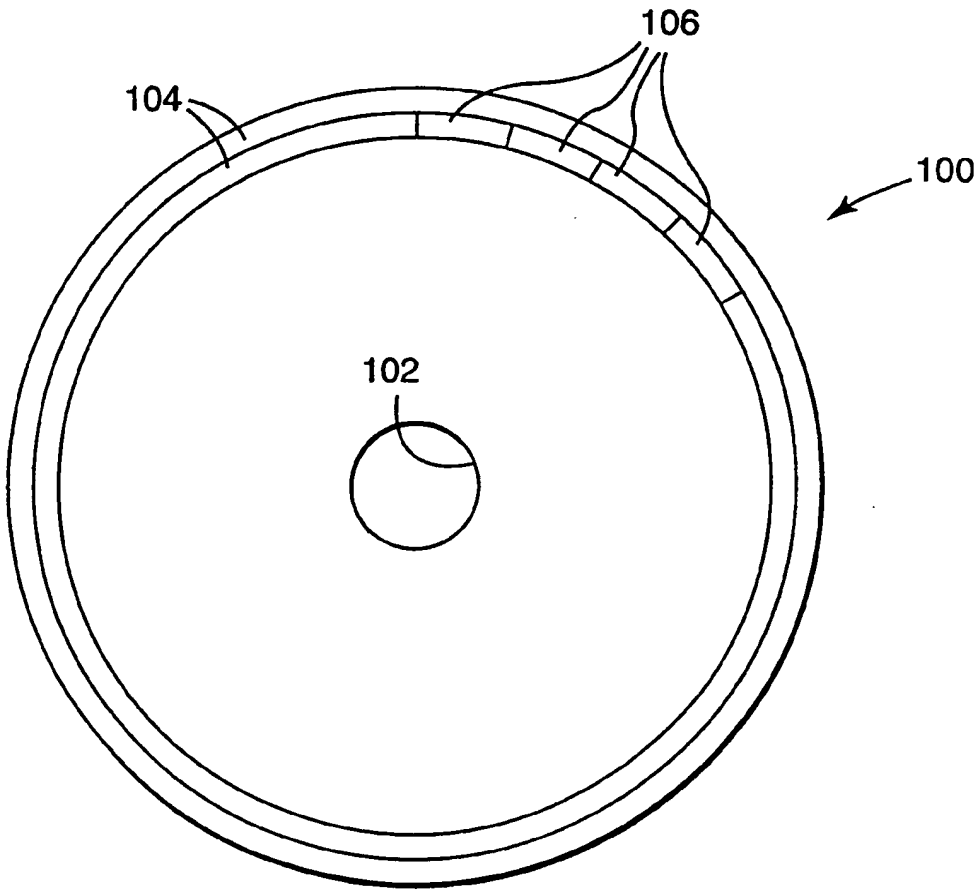


Fig. 1

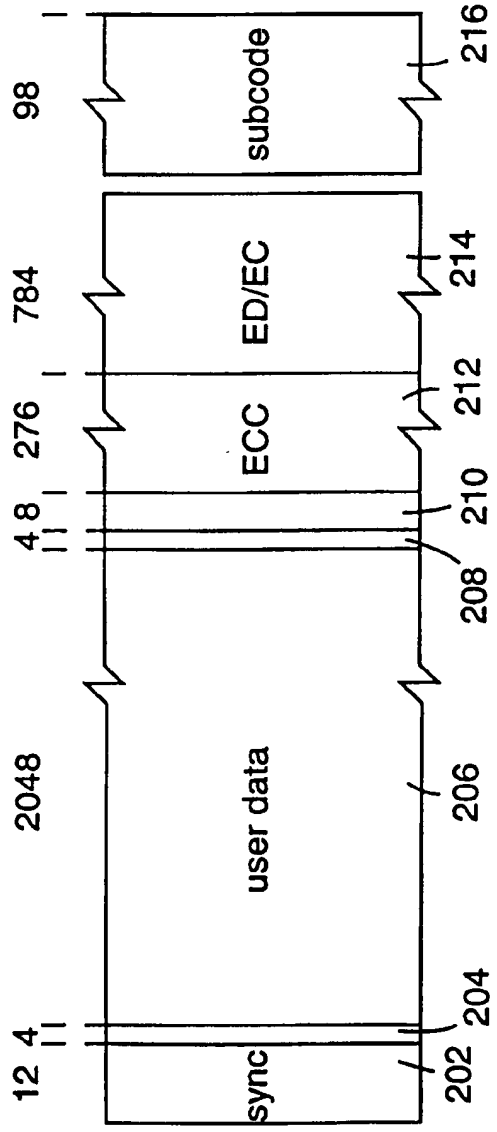

12
4
sync
202
204
2048
user data
206
4
8
208
210
276
ECC
212
784
ED/EC
214
98
subcode
216

Fig. 2A

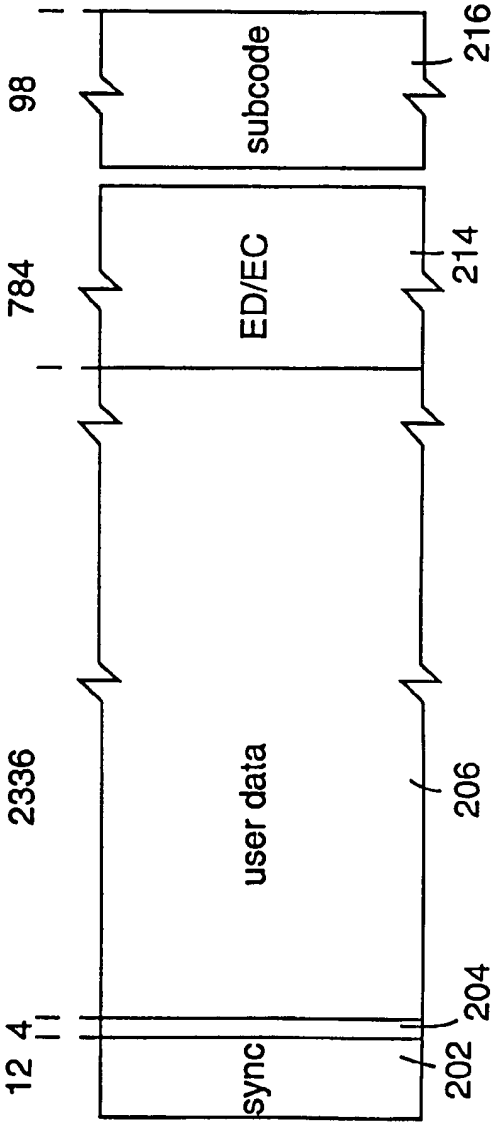

12
4
sync
202
204
2336
user data
206
784
ED/EC
214
98
subcode
216

Fig. 2B

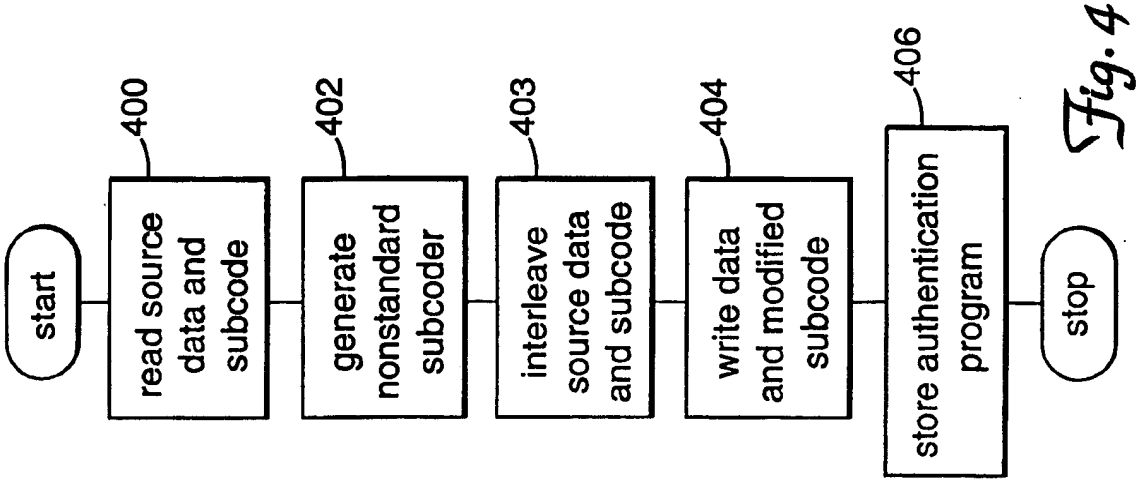

start
read source data and subcode
400
generate nonstandard subcoder
402
interleave source data and subcode
403
write data and modified subcode
404
store authentication program
406
stop

Fig. 4

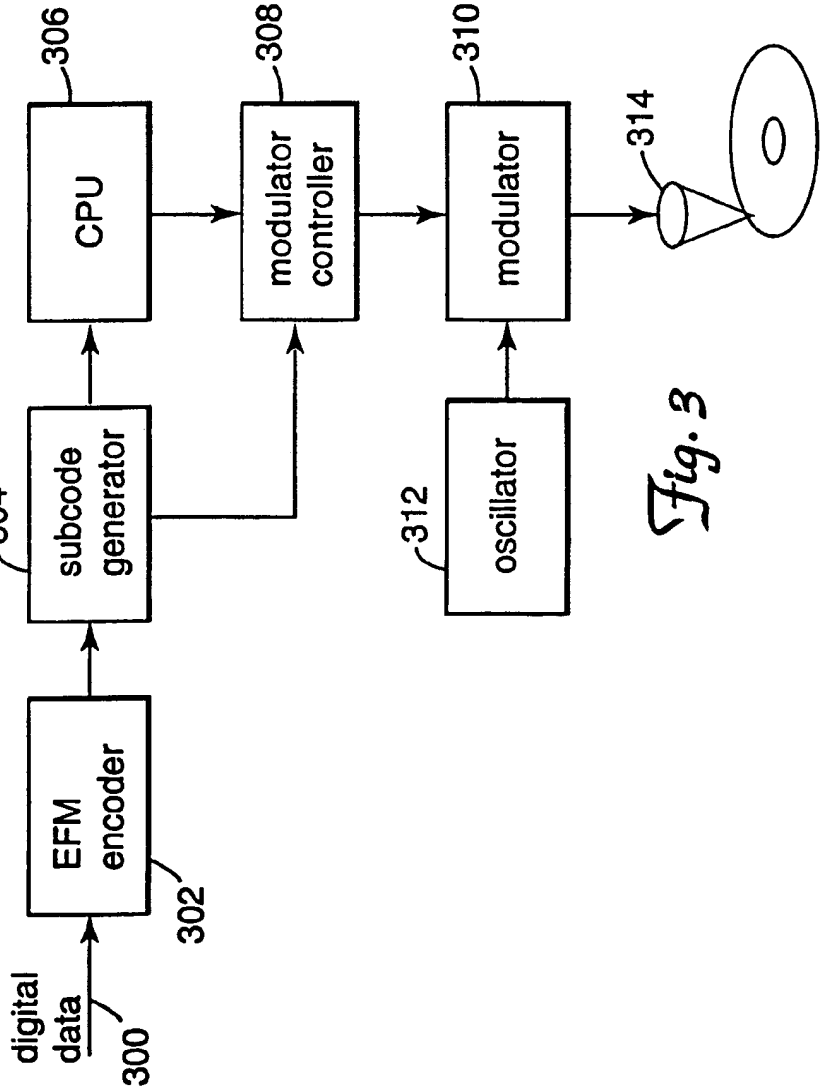

digital data
300
EFM encoder
302
subcode generator
304
CPU
306
modulator controller
308
oscillator
312
modulator
310
314

Fig. 3

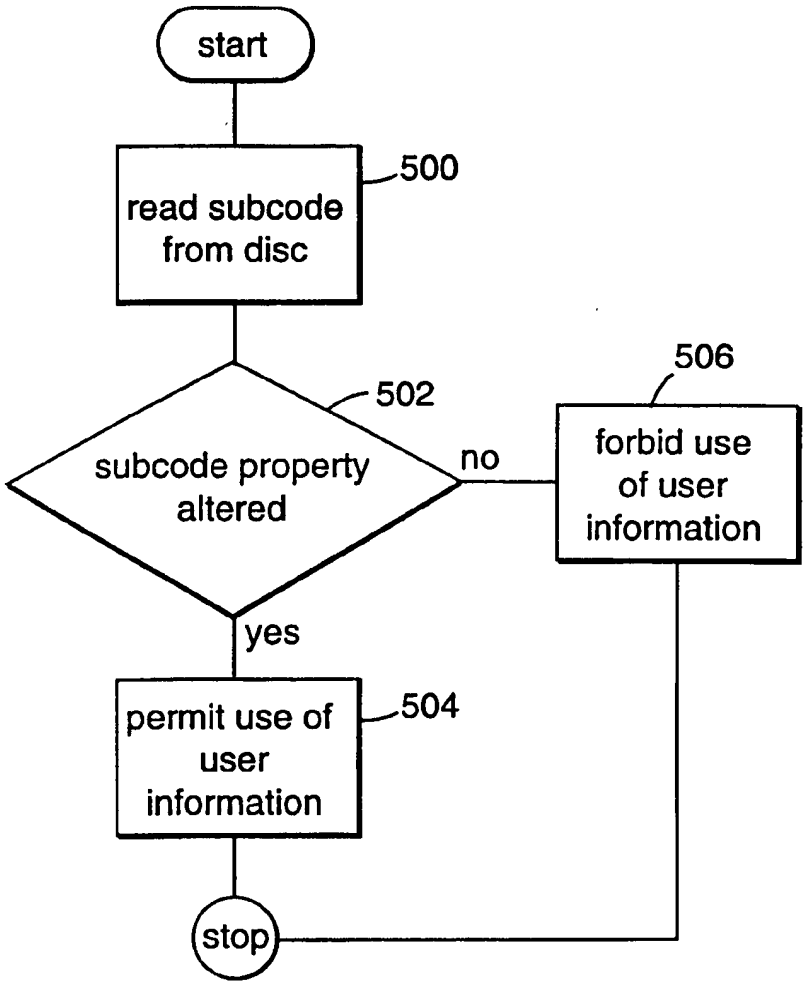

start
read subcode from disc
500
subcode property altered
502
no
forbid use of user information
506
yes
permit use of user information
504
stop

Fig. 5

INTERNATIONAL SEARCH REPORT

Ir ational Application No
PCT/US 98/08422

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 95 03655 A (OAKLEIGH SYSTEMS INC) 2 February 1995 see page 8, line 4 - page 13, line 5; figures 3-6	1,2,4,6, 9-11,13
A	PATENT ABSTRACTS OF JAPAN vol. 096, no. 010, 31 October 1996 & JP 08 153331 A (APPLICS:KK), 11 June 1996 see abstract	1-3
A	PATENT ABSTRACTS OF JAPAN vol. 010, no. 076 (P-440), 26 March 1986 & JP 60 215232 A (NIPPON DENKI KK), 28 October 1985 see abstract	1

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 September 1998	17/09/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Feuer, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/08422

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	PATENT ABSTRACTS OF JAPAN vol. 018, no. 045 (P-1681), 24 January 1994 & JP 05 266575 A (FUJITSU LTD), 15 October 1993 see abstract -----	1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/08422

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9503655 A	02-02-1995	EP 0711479 A	15-05-1996
		US 5596639 A	21-01-1997
		US 5563947 A	08-10-1996